

REMARKS

Claims 1-16 are pending. By this Response, claims 1, 9 and 13 are amended and claim 17 cancelled. Reconsideration and allowance based on the above amendments and following remarks are respectfully requested.

Allowable Subject Matter

Applicants appreciate the indication of claims 6 and 14-16 as being directed to allowable subject matter but are currently objected to as being dependent from a rejected base claim.

Prior Art Rejections

In the Office Action, the Examiner states that claims 1-5, 7-13 and 17 are rejected under 35 U.S.C. §102(e) in view of Rothermel, et al. (US 6,678,827) and Osborne, et al. (US 6,687,833). Applicants respectfully submit that 35 U.S.C. §102 is an anticipatory rejection and cannot be used to reject claims in view of multiple references. It appears that the rejection is meant to be made under 35 U.S.C. §103. However, since a formal rejection under 35 U.S.C. §103 has not been made and a rejection under 35 U.S.C. §102 has been improperly made, applicants respectfully request clarification of the rejection in the next Office Action, if necessary.

In order to expedite prosecution, applicants have provided the following comments with respect to the cited references Rothermel and Osborne and applicant's current amended independent claims 1, 9 and 13.

As amended, claim 1 recites, *inter alia*, a decoy server, functionally coupled to the control system, wherein the apparatus is placed outside a given internal communication network ... taking counter measures against illegal access data received, further wherein the counter measures include providing a response pretending to originate from the internal communication network, the response being sent to a network device within a given internal communication network to be transmitting by the network device to the data communication device.

Claim 9 recites, *inter alia*, taking counter measures against the illegal access data received, wherein the counter measures include providing a response pretending to originate from the internal communication network, the response being sent to a network device within the internal communication network to be transmitted by the network device to the data communication device.

Claim 13 recites, *inter alia*, analyzing the received packet to formulate a response packet, and encapsulating the response packet so that it appears to originate from the target server and sending the encapsulated response packet to a network device, wherein the network device is within the internal network, wherein the network device decapsulates the incapsulated response packet and forwards the decapsulated packet to the source of the unauthorized access packet.

Applicants respectfully submit that at least the above features are not taught by Rothermel and Osborne.

In embodiments of the present invention, an internal network is separately located across the Internet from a decoy server and control system connected to the decoy server. When suspicious data is received at the internal network device and is determined to be an attack by an unauthorized user, the data is incapsualted and sent to the decoy server for handling. The decoy server and control analyze the data and prepare a response to be sent to the attacker. The response is then sent to the internal network from the decoy server. The response is subsequently sent to the attacker from the internal network.

Rothermel teaches a way to remotely manage multiple network security devices. Rothermel discloses utilizing network security devices (NSD) which attempt to control the spread of sensitive information so that only authorized users or devices can retrieve such information. The system monitors network information past between the external network devices and the devices in a group of trusted internal devices. As shown in Fig. 1, the network security devices management system includes a security policy manager device 110 able to communicate with multiple supervisory devices 120 and 160, also referred to as host devices.

Each supervisor device is associated with multiple NSD's with supervisor device 120 associated with NSD's 130-140, and with supervisor device 160 associated with NSD's 161 through 162. Each NSD protects one or more trusted devices from external devices, such as NDS's 130 and 140 protecting devices in internal networks 135 and 145, respectively, from devices external to network 190. See column 1, lines 23 and Fig. 1. In Rothermel, security templates can be created by a user and distributed across multiple NSD's. The security templates provide management information regarding security policies set by the user such that all the NSD's operate under the same policies. See column 4, lines 65 through column 5, line 3.

The Office Action alleges that the security templates correspond to the response data (see page 9 of Office Action). Applicants submit that the templates are not sent to the attacker but are sent to other NSD's. Further, the templates are not response data for an attacker to pretend to originate from an internal network device. The template is created by user to define network policies across multiple NSD's. Thus, the templates cannot correspond to applicant's claimed response data as it is created by a user to define network policies and is not created by a decoy server which prepares a response for an attacker pretending to originate from a particular device. Thus, Rothermel fails to teach sending response data as claimed by applicant's to an attacker.

Osborne is provided to teach the claimed decoy server which is stated in the Office Action as not being taught by Rothermel. Osborne teaches a system in which a virtual host in a network receives data from other parts of network and processes the data perceived to be data from an attacker. The virtual host creates a response to the data and send out the data to the attacker. See column 4, lines 17-20.

The Office Action alleges that the virtual host corresponds to applicant's claimed decoy server. Applicants submit that the virtual host performs the job of sending reply packets to the attacker. This must be performed by the virtual host due to the system design of Osborne. In contrast, applicant's embodiments provide a more universal system in which a decoy server and control system are separate from the internal network. The response created by the decoy server and control are sent to the internal network and the internal network then sends out the response

to the attacker. This is fundamentally different from Osborne's system and provides more dynamic and flexible system allowing the central decoy server and control system to service one or more internal networks.

Thus, Rothermel fails to teach creating a response to send to attackers and Osborne fails to teach sending the response from an internal network device separate from the decoy server. Therefore, the combination of Rothermel and Osborne fail to teach the above noted features of independent claims 1, 9 and 13. Accordingly, reconsideration and withdrawal of the rejection of the claims in view of Rothermel and/or Osborne are respectfully requested.

Conclusion

For at least these reasons, it is respectfully submitted that claims 1-16 are distinguishable over the cited art. Favorable consideration and prompt allowance are earnestly solicited.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Chad J. Billings (Reg. No. 48,917) at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to deposit account no. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

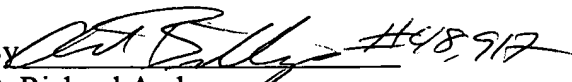
Application No. 09/991,932
Amendment dated September 7, 2006
Reply to Office Action of June 20, 2006

Docket No.: 2565-0238P

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Dated: September 7, 2006

Respectfully submitted,

By  #48,917
to D. Richard Anderson
Registration No.: 40,439
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant